Die militärische Seite der Digitalisierung

von Hans-Jörg Kreowski

Mit Digitalisierung wird üblicherweise ein schon Jahrzehnte anhaltender globaler Prozess bezeichnet, bei dem es sich um den immer noch wachsenden Einsatz von Informations- und Kommunikationstechnik, digitaler Vernetzung, Algorithmisierung, Mediatisierung, Roboterisierung und in letzter Zeit zusätzlich um die Anwendung Künstlicher Intelligenz in nahezu allen gesellschaftlichen Bereichen handelt. Die Digitalisierung hat ihren Ausgangspunkt in der Entwicklung der ersten Computer im Zuge des 2. Weltkriegs und den Jahren danach in Deutschland, Großbritannien und vor allem in den USA, die in enger Verbindung zum militärischen Komplex stattfand. Die ersten Jahrzehnte waren stark vom Geld und von den Anforderungen der Militärs geprägt. Aber auch seitdem der zivile Bereich beginnend in den 1970er und 1980er Jahren insbesondere durch die allmähliche, aber unaufhaltsame Verbreitung von PCs, Notebooks, Laptops, Tablets und schließlich von mobilen Geräten und durch die immer umfassenderen Anwendungen in Wirtschaft, Verwaltung, Bildung und Wissenschaft die Digitalisierung klar dominiert, ist die Verflechtung mit dem Militärwesen nicht verschwunden, sondern ein weiterhin bestimmender Faktor.

Am Anfang war der Krieg

Konrad Zuse hat 1941 mit der Z3 den ersten funktionsfähigen Digitalrechner vorgestellt. Seine Arbeit wurde von der Rüstungsindustrie und staatlichen Stellen gefördert. Als Gegenleistung hat er einen Spezialrechner für die Optimierung der Flügeleinstellungen von Gleitbomben gebaut. Die Computerentwicklung in Großbritannien ist eng mit dem Namen Alan Turing verbunden, der in Bletchley Park an der Entschlüsselung des deutschen Nachrichtenverkehrs mitgewirkt hat. Dafür wurde u.a. der ab 1943 eingesetzte Röhrencomputer Colossus entwickelt.

Entscheidend aber waren mehrere Entwicklungen in den USA. So wurde beispielsweise ab 1942 im Auftrag der US-Armee der Röhrencomputer ENIAC für die Berechnung ballistischer Tabellen gebaut. Solche Tabellen wurden zu Hunderten benötigt, und für jede einzelne musste eine Schar von vor allem Rechnerinnen tagelang arbeiten, was mit ENIAC tausendmal schneller ging. Eine Parallelentwicklung im Auftrag der US-Marine ab 1945 war Whirlwind. Ursprünglich für Flugsimulation gedacht, wurde es später im SAGE-System eingesetzt, das erste computergestützte Luftverteidigungssystem. Weitere Durchbrüche gelangen durch die Erfindung der Transistoren, die die ausfallanfälligen Röhren ersetzten, und der integrierten Schaltungen, die eine lange Phase der Miniaturisierung und Verkürzung der Rechenzeiten einläuteten. Das kulminierte von 1980 bis 1990 im milliardenschweren Very High Speed Integrated Circuits program (VHSIC) des US-Verteidigungsministeriums. Ziel war, die Grenzen zu verschieben, die die Hardware den militärischen Systemen setzte.[1]

Softwarekrise

Bei der Entwicklung großer Softwaresysteme, wie sie insbesondere für militärische Anwendungen in den 1950er und 1960er Jahren gefordert waren, stellte sich bald heraus, dass sie häufig viel teurer wurden als geplant, dass das Projektmanagement nicht klappte und dass die Zuverlässigkeit erheblich zu wünschen übrig ließ. Während die Hardware kontinuierlich verbessert wurde, wurden die Softwareprobleme immer größer. Es gab ab den späten 1960er und vor allem in den 1970er und 1980er Jahren zwei große Anstrengungen, diese sogenannte Softwarekrise zu beheben, bei denen die im Entstehen begriffene wissenschaftliche Disziplin der Informatik um Mithilfe gebeten wurde. Zum einen setzte das US-amerikanische Verteidigungsministerium die Entwicklung der Programmiersprache ADA in Gang, die mehrere hundert bis dahin benutzte Programmiersprachen ersetzen sollte.[2] Zum anderen lud die NATO zu mehreren internationalen Konferenzen ein, auf denen das inzwischen ganz zentrale

Fachgebiet der Softwaretechnik aus der Taufe gehoben wurde mit dem Ziel methodisch fundierter Systementwicklung. Die Einführung von ADA im Laufe der 1980er Jahre hat zwar zu einer erheblichen Reduktion des (Programmier-)Sprachwirrwarrs geführt, und ADA wird bis heute in sicherheitskritischen, vor allem auch militärischen Bereichen verwendet, der erhoffte durchschlagende Erfolg ist aber ausgeblieben. Im Laufe der 1980er Jahre wurde vom US-amerikanischen Verteidigungsministerium auch noch ein weiteres Großprojekt aufgelegt, das in den ersten vier Jahren ein Budget von über 140 Mio. US-Dollar hatte: Software Technology for Adaptable Reliable Systems program (STARS).[3] In der Softwaretechnik hat es erhebliche Fortschritte gegeben, wobei der immense Bedarf an Softwareentwicklung im zivilen Bereich mitausschlaggebend war. Die Softwareprobleme sind allerdings nicht verschwunden, denn die Anforderungen an Software sind sowohl militärisch als auch zivil eher noch stärker gewachsen als der methodische Fortschritt.

Aufrüstung zum Informations- und Cyberkrieg

Krieg zu führen geht weit über Töten und Zerstören durch Waffeneinsatz hinaus. Krieg ist ein komplexes Organisationsmonster, zu dem Aufklärung und Geheimhaltung, Propaganda, Spionage und Sabotage, Kommando, Kontrolle und Kommunikation gehören. Durch die Digitalisierung sind die Mittel und Möglichkeiten in all diesen Bereichen erheblich gewachsen. Fast alle Länder der Welt haben Cyberkriegseinheiten gebildet, die Konzepte und Programmsysteme entwickeln, wie man Falschmeldungen streut, um breit angelegte Desinformationskampagnen zu starten, wie man Gegner (und oft auch Verbündete) ausspioniert und wie man kritische Infrastrukturen ausschaltet bis hin zur Zerstörung technischer Einrichtungen. Die jüngsten Enthüllungen eines Recherche-Netzes des ZDFs, der Süddeutschen Zeitung, des Spiegels u.a. zeigen, wie das IT-Unternehmen NTC Vulkan zusammen mit russischen Geheimdiensten im großen Maßstab Cyberkrieg plant. Explizit genannt sind das Lahmlegen von Kontrollsystemen von Eisenbahn-, Luft- und Schiffstransport und die Störung von Energieunternehmen. Wenn auch diese Vulkan Files ziemlich erschrecken, muss man bedenken, dass nicht nur Russland in diesem Bereich aufrüstet. So hält die NATO schon seit vielen Jahren jährliche Manöver ab, bei denen offensiv und defensiv ähnliche Cyberkriegsszenarien geübt werden. Dass es sich dabei nicht nur um Planungen handelt, zeigt eine lange Liste von Cyberangriffen mit gravierenden Auswirkungen. Dass zivile Infrastrukturen durch Cyberattacken besonders gefährdet sind und sie als bevorzugte Ziele gelten, ist kriegsvölkerrechtlich im höchsten Maße bedenklich. Die NATO ist sich dessen auch voll bewusst. Sie hat eine Studie zur Anwendung des Kriegsvölkerrechts auf Cyber-Konflikte und Cyberkrieg in Auftrag gegeben, an der seit 2009 rund 20 Fachleuten am NATO Cooperative Cyber Defence Centre of Excellence in Tallinn gearbeitet haben.[4]

Künstliche Intelligenz im Kriegsdienst[5]

1956 trafen sich zwölf junge Wissenschaftler für mehrere Wochen und hoben das Gebiet der Künstlichen Intelligenz (KI) aus der Taufe. Erklärtes Ziel war es, kognitive Fähigkeiten wie Sehen und Erkennen, Hören und Verstehen, Planen und Entscheiden sowie Problemlösen mit Hilfe von Computerprogrammen zu simulieren. Das fand seine Grenzen aber insbesondere in der damals noch sehr begrenzten Speicherkapazität und Rechengeschwindigkeit. Dennoch hat das US-Verteidigungsministerium prinzipiell das militärische Potenzial der KI erkannt und 1983 die Strategic Computing Initiative (SCI) gestartet,[6] wobei drei Aufgaben im Zentrum standen: ein Sprachassistent für die Piloten der Luftwaffe, ein Schlachtenmanagementsystem für die Marine und autonome Landfahrzeuge für das Heer. SCI war auf zehn Jahre angelegt und hatte einen für damalige Verhältnisse gigantischen Finanzrahmen von fast einer halben Milliarde US-Dollar. Da sich keine schnellen Erfolge abzeichneten, wurde das Programm noch vor dem Ende gekürzt. Dennoch muss SCI wohl als Ausgangspunkt einer beispiellosen Entwicklung der KI gesehen werden. Inzwischen hat die Verarbeitung von Sprache und Text ein unglaubliches Niveau erreicht, genauso wie die Verarbeitung von Bildern, wie sie insbesondere für das eigenständige Navigieren von Fahrzeugen benötigt wird. Und Managementsysteme sind inzwischen weit verbreitet. Dabei ist festzuhalten, dass sich die Ziele und auch die Methoden seit den Anfängen der KI gar nicht allzu sehr verändert haben, aber der heute verfügbare Speicherplatz und die Rechengeschwindigkeit erlauben solche Anwendungen. Während sich unbemenschte Land- und Wasserfahrzeuge auch nach Jahrzehnten intensiver Entwicklung immer noch in einer Art Pilotphase befinden, sind die entsprechenden fliegenden Systeme bereits seit 20 Jahren im Einsatz. Angefangen hat es mit Aufklärungsdrohnen, die feindliches Gebiet überfliegen und ausspionieren können. Es hat dann nicht lange gedauert, bis solche Drohnen mit Raketen ausgestattet wurden. Vorreiter waren Israel und die USA. Inzwischen sind Killerdrohnen weit verbreitet, und es gibt sie in einer breiten Palette von klein bis groß und von billig bis teuer. Zu den Herstellerstaaten gehören u.a. China, Iran, Russland und die Türkei. Mehrere Dutzend Staaten haben diese Waffen angeschafft und setzen sie teilweise auch

bereits ein. Nachdem es Tausende Einsätze in Afghanistan, Pakistan, Jemen und andernorts in eher asymmetrischen Kriegen mit vielen Ziviltoten gegeben hat, zeigt der Krieg in der Ukraine, dass bewaffnete Drohnen auch eine Rolle spielen, wenn zwei Armeen gegeneinander kämpfen. Aufklärungs- und Killerdrohnen sind Waffensysteme, die es ohne Digitalisierung nicht gäbe, weil sie programmgesteuert fliegen und vor allem, weil sie ihre Ziele mithilfe digitaler Bildverarbeitung finden. Der nächste Entwicklungsschritt, an dem intensiv gearbeitet wird, ist die vollständige Autonomie, bei der dann die Bordsysteme auch über den Waffeneinsatz entscheiden. In Politik und Militär sind autonome Waffen aus ethischer und kriegsvölkerrechtlicher Sicht nicht unumstritten, ein Verbot ist dennoch nicht absehbar.[7]

Die Cyberpeace-Kampagne

Die Gründung des Forums InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF) 1984 auf dem Höhepunkt der Friedensbewegung war eng verbunden mit dem NATO-Doppelbeschluss zur Nachrüstung mit Mittelstreckenraketen in Europa und hing zusammen mit der Kampagne verschiedener insbesondere universitärer Friedensinitiativen Informatiker warnen vor einem Atomkrieg aus Versehen. Die unheilvolle Verquickung von Rüstung und Informatik war fortan bestimmendes Thema im FifF, anfangs getragen von einem äußerst aktiven Arbeitskreis. Einen besonderen Schub hat die Thematik 2013 bekommen, als das FIfF die Cyberpeace-Kampagne startete. Edward Snowden hatte gerade durch seine Enthüllungen einer breiten Öffentlichkeit offenbart, dass die NSA (und ähnlich andere Geheimdienste) weltweit die digitale Kommunikation ausspionieren. Das FIfF wollte darauf aufmerksam machen, dass die Problematik nicht nur Grund- und Menschenrechte unterminiert, sondern dass mit ganz ähnlich gelagerten Methoden auch massiv zum Cyberkrieg gerüstet wird. Cyberpeace war gedacht als Gegenkonzept. Die Kampagne umfasste vor Corona eine Vielzahl von Publikationen, Veranstaltungen und Aktionen. Eine besondere Errungenschaft wurde durch Fördermittel der bridge-Stiftung möglich: In Zusammenarbeit mit dem Motionensemble entstand 2017 das Video Cyberpeace statt Cyberwar, das bei vimeo oder youtube angesehen werden kann. Ein Kern der Kampagne war die Entwicklung von 14 Forderungen an die Politik, zu denen eine rein defensive Sicherheitsstrategie durch Verbot von Offensivwaffen für den Cyberkrieg und eine digitale Genfer Konvention mit dem Verbot von Cyberangriffen auf lebenswichtige Infrastrukturen wie Strom-, Wasser-, Gesundheitsversorgung etc. gehört. Es geht um die ausschließlich zivile Nutzung des Internets und aller digitalen Medien.[8] Da die Thematik nichts an Aktualität und Brisanz eingebüßt hat, hat das FIfF begonnen, der Cyberpeace-Kampagne neuen Schwung zu verleihen. Wer mitwirken möchte, ist herzlich willkommen.

Anmerkungen

1 Näheres dazu siehe „The History of the Integrated Circuit“. Nobelprize.org. Nobel Media AB 2014. Web. 29 Jun 2018.

2 Näheres dazu siehe de.wikipedia.org/wiki/Ada_(Programmiersprache).

3 Näheres dazu siehe Larry F. Druffel, Samual T. Redwine Jr. and William F. Riddle: The DoD Stars Program. Computer, vol. 16, no. 11, pp. 9-11, 1983. doi: 10.1109/MC.1983.1654232.

4 Das Tallinn Manual erschien 2013 und Tallinn 2.0 2017, beide bei Cambridge University Press. Während es in Teil 2 um Einzeloperationen geht, behandelt Teil 1 massivste Cyber-Operationen in bewaffneten Konflikten oder bei verbotenem Gewalteinsatz in internationalen Beziehugen.

5 Für eine ausführliche Darstellung des Themenkomplexes siehe Hans-Jörg Kreowski und Aaron Lye (Hrsg.): Künstliche Intelligenz zieht in den Krieg, Schwerpunkt. FIfF-Kommunikation 4/2021, S. 28-30 und Dossier 93, Beilage zu Wissenschaft und Frieden 4/2012.

6 Näheres dazu siehe Alex Roland and Phlip Shiman: Strategic Computing - DARPA and the Quest for Machine Intelligence, 1983-1993. The MIT Press 2002.

7 Zu militärischen, völkerrechtlichen und wissenschaftlichen Aspekten autonomer Waffensysreme siehe Andrew P. Williams and Paul D. Scharre (Eds.): Autonomous Systems – Issues for Defence Policymakers.NATO Headquarters Supreme Allied Commander, Transformation, Norfolk, Virginia, United States.

8 Detaillierte Informationen zur Cyberpeace-Kampagne findet man auf der Webseite cyberpeace.fiff.de.